METHOD FOR AUTOMATICALLY CONFIGURING A DSLAM TO RECOGNIZE CUSTOMER PREMISES EQUIPMENT

TECHNICAL FIELD OF THE INVENTION

This invention relates in general to telecommunications, and more particularly to a method for automatically configuring a DSLAM to recognize customer premises equipment.

BACKGROUND OF THE INVENTION

Digital subscriber line add/drop multiplexers (DSLAMs) receive information from a variety of customer premises and communicate that information to a backbone network. In order to receive information from customer premises, DSLAMs must be configured to recognize the customer premises equipment from which the information is being received. One solution for configuring the equipment is to maintain a table of information on the available connections at DSLAM. Customer premises equipment may then be manually configured based on the assignment scheme in the table. A drawback to this method is that it requires a visit to the customer premises, and it also requires information about the available connections on the DSLAM. Accordingly, there is a need for a method that would allow DSLAMs to be configured automatically to recognize customer premises equipment.

SUMMARY OF THE INVENTION

In one embodiment, a method for automatically configuring a digital subscriber line add-drop multiplexer (DSLAM) includes receiving a request for a connection with unrecognized customer premises equipment at a DSLAM, establishing the connection between the DSLAM and the customer premises equipment, and associating the connection with a status having three possible states, which include an unverified state, a verified state, and an invalid state. The verified state indicates that the connection is allowed full access to a network, the unverified state indicates that the connection is allowed conditional access to the network, and the invalid state indicates that the connection is not allowed to access the network. The method further includes setting the status of the connection to unverified and authenticating the unrecognized customer premises equipment. If the unrecognized customer premises equipment is authenticated, the method includes setting the status of the connection to verified. If the unrecognized customer premises equipment is not authenticated, the method includes setting the status of the connection to invalid. The method also includes providing access to the network according to the current status of the connection.

In another embodiment, a digital subscriber line add-drop multiplexer (DSLAM) includes an interface, a memory, and a processor. The interface receives a request for a connection with unrecognized customer premises equipment and establishes the connection with the unrecognized customer premises equipment. The memory stores a connection identifier and a status for the connection. The status has three possible states, which include an unverified state, a verified state, and an invalid state. The verified state indicates that the connection is allowed full access to a network, the unverified state indicates that the connection is allowed conditional access to the network, and the invalid state indicates that the connection is not allowed to access the network. The processor sets the status of the connection as unverified when the connection is established and authenticates the unrecognized customer premises equipment. The processor sets the status of the connection as verified if the customer premises equipment is authenticated, sets the status of the connection as invalid if the customer premises equipment is not authenticated, and provides access to the network according to the current status of the connection.

Important technical advantages of certain embodiments of the present invention include automatic configuration of a DSLAM. Certain embodiments of the present invention allow a DSLAM to recognize customer premises equipment connected to the DSLAM without requiring manual configuration of the customer premises equipment to recognize the DSLAM. This reduces time and expense associated with setting up customer premises equipment. It also increases the versatility of DSLAM, because customer premises devices may be changed out without requiring configuration to DSLAM.

Other important technical advantages of certain embodiments of the present invention include multicasting from the DSLAM. As DSLAM is configured to recognize different customer premises equipment, DSLAM can maintain a table of connections. This table may subsequently be used to broadcast information to all customer premises equipment coupled to DSLAM. Consequently, DSLAM may be used to communicate broadcasts even when the particular customer premises equipment to receive the information is not known. These cases would occur more frequently when customer premises equipment is not previously configured, and DSLAM may not have information that would normally be input during configuration.

Other technical advantages of the present invention will be readily apparent to one skilled in the art from the following figures, descriptions, and claims. Moreover, while specific advantages have been enumerated above, various embodiments may include all, some, or none of the enumerated advantages.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention and its advantages, reference is now made to the following description, taken in conjunction with the accompanying drawings, in which:

FIGURE 1 shows a communications network that includes customer premises equipment coupled to a DSLAM;

FIGURE 2 shows one embodiment of a DSLAM that includes configuration tables;

FIGURE 3 is a configuration table that may be maintained at a DSLAM;

FIGURE 4 is a flowchart that illustrates an example method for automatic configuration of a DSLAM; and

FIGURE 5 is a flowchart illustrating an example method for broadcasting information to recognized customer premises equipment.

DETAILED DESCRIPTION OF EXAMPLE EMBODIMENTS OF THE INVENTION

FIGURE 1 illustrates a network 100 that includes a digital subscriber line add/drop multiplexer (DSLAM) 101 coupled to several customer premises 102. At each of the customer premises 102 is customer premises equipment 104 that communicates with DSLAM 101. Customer premises equipment allows communication devices 105 at customer premises 102 to communicate with a backbone network 114 through DSLAM 101. DSLAM 101 thus provides access to backbone network 114 to communication devices 105. Backbone network 114 may communicate information in any suitable form, such as packets, cells, frames, segments, or other portions of information, using any suitable communication method, such as transfer control protocol / Internet protocol (TCP/IP), Ethernet, synchronous optical network (SONET), and/or asynchronous transfer mode (ATM).

DSLAM 101 includes any hardware and/or software for receiving information from customer premises equipment 104 and communicating information to backbone network 114. In a particular embodiment, DSLAM 101 receives information from customer premises equipment 104 in the form of asynchronous transfer mode (ATM) cells communicated over DSL. In this embodiment, DSLAM 101 extracts ATM cells from DSL signals using a DSL digital signal processor (DSP) 106. A segmentation and reassembly module (SAR) 108 extracts information ATM cells and converts it into a format suitable for use by backbone network 114. Control processor 110 may also assist in the process by rearranging information extracted from ATM cells, appending or removing headers, or performing any other information processing useful for making the information suitable for routing to backbone network 114. Packet processor 112 receives information from SAR 108 and control processor 110 in the form of packets and communicates information to backbone network 114. SAR 108, control processor 110, and packet processor 112 generally describe functional modules of DSLAM 101, but it should be understood that the functions performed by these particular components may be distributed among several components or consolidated within shared components without substantially changing the operation of DSLAM 101.

Customer premises equipment 104 represents any suitable hardware and/or software for receiving information from communication devices 105 and communicating this information in a suitable format to DSLAM 101. Customer premises equipment 104 may perform any suitable conversion, formatting, or processing of information from communication devices 105. Communication devices 105 may include any form of device that exchanges information using backbone network 114. Communication devices 105 may include personal computers, peripherals, internet protocol telephones (IP phones), hubs, routers, or other suitable devices. Information sent from customer premises equipment 104 is associated with some identifying information indicating the origin of the information. In a particular embodiment, customer premises equipment 104 communicates ATM cells over DSL. In such an embodiment, the identifier for the information could be a virtual channel identifier (VCI) or virtual path identifier (VPI).

Customer premises equipment 104 also extracts information from ATM cells received from DSLAM 101. In one example, DSLAM 101 receives information intended for customer premises equipment 104 from backbone network 114. Packet processor 112 passes the information to SAR 108, which looks up the appropriate destination for the information. Alternatively, SAR 108 may broadcast information to several customer premises 102 if the destination of the information is unknown. SAR 108 converts packet information from backbone network 114 into ATM cells along with appropriate identifiers associated with the destination customer premises equipment 104. These ATM cells are sent to DSL DSPs 106 which convert the ATM cells into DSL signals that are communicated to customer premises equipment 104.

In operation, customer premises equipment 104 communicates information to DSLAM 101. If customer premises equipment 104 has previously communicated with DSLAM 101 and has been recognized by DSLAM 101, then information exchange takes place in the normal manner described above. However, if customer premises equipment 104 is not recognized by DSLAM 101, then DSLAM 101 treats the channel from which the information was received as "unverified." This status indicates that customer premises equipment 104 has not yet been recognized by DSLAM 101. Control processor 110 may then verify whether the information received from customer premises equipment 104 from the unverified connection is authorized to be sent to backbone network 114. If the information is authorized, SAR 108 updates a configuration table to associate a VCI for the customer premises equipment 104 with the authenticated connection. Once that has taken place, the connection is then considered "verified," and subsequent information received over that connection will be sent normally. Thus, DSLAM 101 may configure itself to recognize customer premises equipment 104 even when customer premises equipment 104 has not been programmed with information about how DSLAM 101 has been configured.

FIGURE 2 shows one embodiment of DSLAM 101. In the depicted embodiment, DSLAM 101 includes a processor 202, an interface 204, and a memory 206. Processor 202 represents any hardware and/or software component useful for processing information and performing various tasks of DSLAM 101. In a particular embodiment, processor 202 performs any suitable tasks of SAR 108, control processor 110, or packet processor 112 described above.

Interface 204 represents any port or connection suitable for exchanging information with backbone network 114 and/or customer premises equipment 104. In a particular embodiment, interface 204 may include physical layer devices such as DSL DSPs 106, as well as suitable connections for communicating information to backbone network 114. The functions performed by interface 204 may be distributed among several different hardware or software components of DSLAM 101, or may be consolidated within shared components.

Memory 206 represents any suitable form of information storage for DSLAM 101. Memory 206 may include magnetic media, optical media, removable media, local storage, remote storage, or any other suitable information storage medium. Memory 206 stores code 208, which represents instructions executed by processor 202 to perform various tasks of DSLAM 101. Memory 206 also stores connection table 210. Connection table 210 maintains information on the status of particular connections formed by DSLAM 101 with customer premises equipment 104. Connection table 210 also maintains a status for each connection so that DSLAM 101 may recognize whether the information received from customer premises equipment 104 is verified, unverified, or invalid. Invalid connections are unauthorized attempts to communicate information to backbone network 114, and accordingly, information from those connections is discarded.

In operation, DSLAM 101 receives information from customer premises equipment 104 which is converted into a suitable form by interface 204. Processor 202 then determines based on the information in connection table 210 whether any information has previously been received from this connection. If information has not previously been received from this connection, processor 202 may create a new entry in connection table 210 that indicates that the connection is unverified. If information is received from a verified connection, processor 202 may forward the information to backbone network 114 using interface 204. If information is received from a connection that has already been determined to be invalid, then processor 202 may discard the information. For unverified connections, processor 202 may store packets in a buffer 212 in memory 206 while it is being determined whether the connection is valid or not.

Processor 202 also determines whether a connection is valid. To do so, processor 202 compares authentication in the information received from customer premises equipment 104 to information stored in memory 206. If the information is not authenticated, processor 202 may treat the connection as invalid and appropriately update connection table 210. On the other hand, if information is authenticated, processor 202 may update connection table 210 to reflect that the connection has been verified.

DSLAM 101 may also receive information from backbone network 114. In this case, processor 202 receives data from interface 204. Processor 202 analyzes the information to determine destination customer premises equipment 104 for the information. To send information to customer premises equipment 104 with a known destination, processor 202 looks up the appropriate customer premises equipment 104 in connection table 210, and communicates the information to customer premises equipment 104 using interface 204. Alternatively, if there is no recognized destination, processor 202 may broadcast the information. If no destination is specified or if the identity of the destination is unclear from connection table 210, processor 202 may copy the packet or other information received, and communicate it to each customer premises equipment 104 identified in connection table 210. Packets may be buffered in buffer 212 before they are communicated to customer premises equipment 104.

FIGURE 3 is one example of a connection table 210 used by certain embodiments of DSLAM 101. In the depicted embodiment, each connection is identified by a VCI 212. Table 210 associates particular information about each connection with VCI 212. For each connection, table 210 includes a status 214. Status 214 indicates whether each connection is verified, unverified, or invalid. A verified connection is a connection that has been authenticated according to an appropriate security procedure so that customer premises equipment 104 associated with that connection is authorized to send information to backbone network 114. An unverified connection is a connection that has been established with customer premises equipment 104 that has not yet been authenticated by DSLAM 101. Such a connection takes place when customer premises equipment 104 initiates a connection with DSLAM 101. An invalid connection is a connection associated with customer premises equipment 104 that has failed the authentication procedure and therefore is not authorized to communicate information to network 114.

During operation, DSLAM 101 updates table 210 to reflect new information about particular connections. When DSLAM 101 initially accepts a connection with customer premises equipment 104, DSLAM 101 generates an entry for table 210 with unverified status 214. While a connection is active, DSLAM 101 maintains context 216 for each connection. Context 216 tracks usage information for each connection, such as the number of cells sent or received over the connection.

After the connection is established, DSLAM 101 attempts to determine whether the particular customer premises equipment 104 forming the connection is authorized for network 114. If customer premises equipment 104 is not authorized, DSLAM 101 updates status 214 for that connection to invalid. Subsequent information from that connection may then be discarded by DSLAM 101, and DSLAM 101 may exclude that connection from any broadcasts. The connection may also be terminated. DSLAM 101 may also maintain invalid status 214 for the connection in table 210, so that subsequent attempts by unauthorized customer premises equipment 104 to establish a connection may be rejected.

On the other hand, if customer premises equipment 104 is authenticated, then DSLAM 101 updates status 214 for the connection to verified. DSLAM 101 permits customer premises equipment 104 on a verified connection to exchange information freely with network 114. DSLAM 101 may also include verified connections in subsequent broadcasts to customer premises equipment 104. By contrast, information from unverified connections may be buffered or otherwise kept from network 114 until the connection is verified. Similarly, DSLAM 101 may exclude unverified connections from broadcasts.

FIGURE 4 is a flow chart 400 that illustrates an example method for automatically recognizing customer premises equipment 104 at DSLAM 101. DSLAM 101 receives a connection request from unrecognized customer premises equipment 104 at step 402. DSLAM 101 buffers information received over that connection at step 404 and sets status 214 for the connection as unverified at step 406.

DSLAM 101 then authenticates unrecognized customer premises equipment 104 at step 408. If customer premises equipment 104 is authorized, DSLAM 101 sets status 214 as verifies and communicates buffered information to network 114. DSLAM 101 then maintains the connection at step 414, allowing information to be sent back and forth between customer premises equipment 104 and network 114. DSLAM 101 may also maintain context 216 for the connection. The connection may be maintained until ended, as shown by decision step 416.

If customer premises equipment 104 is unauthorized, DSLAM 101 sets status 214 for the connection as invalid at step 418. DSLAM 101 may then terminate the connection at step 420, or alternatively, may maintain the connection and allow customer premises equipment 104 one or more additional attempts to verify its authorization. If a connection is terminated, any buffered packets and subsequent packets received from the invalid connection may be discarded. DSLAM 101 may maintain status 214 of the connection so that subsequent attempts by invalid customer premises equipment 104 to re-establish the connection may be ignored.

FIGURE 5 is a flow chart 500 that illustrates an example method for broadcasting messages to customer premises equipment 104. DSLAM 101 receives a packet from network 114 at step 502. DSLAM 101 determines whether a destination indicated by the packet is known and verified at step 504. For example, DSLAM 101 may consult table 210 to determine whether a particular connection is active that corresponds to the destination of the packet. If DSLAM 101 recognizes the destination as a verified connection, DSLAM 101 communicates the packet to the destination at step 506. If DSLAM 101 recognizes the destination as being associated with an invalid connection, DSLAM 101 may discard the packet at step 507.

If the destination is unknown to DSLAM 101, DSLAM 101 may broadcast the information in the packet to known and verified destinations. DSLAM 101 selects a first connection in table 210 at step 508. DSLAM 101 determines status 214 for the connection at step 510. Based on the status, DSLAM 101 determines whether the connection is verified at step 512. If the connection is verified, DSLAM 101 copies the packet at step 514 and communicates the packet to customer premises equipment 104 using the verified connection at step 516. Otherwise, DSLAM 101 does not send the packet to unverified or invalid customer premises equipment 104. Steps 508 through 518 may be repeated for the remaining connections in table 210, as shown in decision step 518.

The particular methods of operation described in FIGUREs 4 and 5 are only examples, and it should be understood that different embodiments of DSLAM 101 may use different methods of operation. For example, DSLAM 101 may allow customer premises equipment 104 on unverified connections to exchange information with network 114 and receive broadcasts before customer premises equipment 104 is authenticated. It should be understood that other methods of operation, and in particular, any method of operation consistent with any part of the description found above, may also be performed by DSLAM 101.

Although the present invention has been described with several embodiments, a myriad of changes, variations, alterations, transformations, and modifications may be suggested to one skilled in the art, and it is intended that the present invention encompass such changes, variations, alterations, transformations, and modifications as fall within the scope of the appended claims.